The RFID Guardian User Interface

on mobile devices

RFID Guardian

Application manual

Table of Contents

Table of contents 2

1. About This Document 4

1.1 Purpose 4

1.2 Compatibility 4

1.3 Audience 4

2. Installation – Get started 5

3. Main Menu – Application overview 6

3.1 Tags 7

3.2 Readers 7

3.3 Access Control 7

3.4 Auditing 7

3.5 Advanced 7

3.6 Connect to Guardian 7

4. Connect to the RFID Guardian 8

5. Tags 11

5.1 Conduct RFID scan 11

5.2 Transfer ownership of tags 11

5.3 Manage Tag Lists 11

5.3.1 Set management 12

5.3.2 *Present* Tags 14

5.3.3 *All* Tags 14

5.3.4 Add – Delete Tags 16

5.4 Key management 16

5.5 Tag spoofing 18

6. Readers 20

6.1 List of Readers 20

6.2 List of Roles 22

6.3 Key management 24
6.4 Add/Remove reader 25
6.5 Create/Delete role 25
7. Access Control 26
7.1 Access Control List rules (ACL rules) 26
7.1.1 Select ACL directory 26
7.1.2 Check ACL status 28
7.1.3 ACL reload 28
7.1.4 ACL save 28
7.1.5 Clear ACL 28
7.2 ACL Contexts 29
8. Auditing 30
9. Advanced 32
9.1 Security 32
9.2 Configuration 32
9.2.1 Authentication 33
9.2.2 Key management 33
9.2.3 Access Control 33
9.2.4 Auditing 33
9.2.5 System time 33
9.3 Administration 34
9.3.1 Load new programs 35
9.3.2 Reflash EEPROM 35
9.3.3 Clean up the filesystem 35
9.3.4 Backup 35
9.3.5 Synchronize 35
9.3.6 Phone Browser 35
9.3.7 Guardian Browser 37

1. About This Document

1.1 Purpose

This document gives an overview of the RFID Guardian user interface and describes the potential communication between an RFID Guardian and a mobile device that runs the application to control the Guardian.

1.2 Compatibility

The software documented here is compatible with (up to) the V3 of the RFID Guardian.

The devices on which the software runs, should support the Mobile Information Device Profile 2.0 (**JSR 118**), as well as have Bluetooth connectivity (**JSR 82**) and provide file system access (**JSR 75**).

From the hardware point of view, a five-way navigation key and two soft keys are necessary for the device. The application is indepentent of the keyboard type; however, a full (QWERTY) keyboard would make use of it easier, in cases where the user has to input some text.

The software was tested on two **S60 3rd edition**, Nokia devices; all screenshots in this document are taken from those devices and are used to give a clear view of how the application is used in practice.

1.3 Audience

This document is intended, in the first place, for people who possess an RFID Guardian and an appropriate mobile device, and want to know how to use the application to control the Guardian.

It will also help other persons to get a general view of the RFID Guardian user interface for mobile devices, what it is and what it can do.

2. Installation – Get started

To get the application (RFID Guardian user interface for mobile devices) on your mobile device, visit www.rfidguardian.org/rfid.jar . The installation process is similar to any other application's installation process. For more information, check the user guide of your mobile device.

After the application is installed, you are ready to start using it. Select ***Menu > Installations*** on your device, and start the "RFID Guardian" application. In the following pages, it is supposed that the steps described in this section have already been followed by the user.

Image 2.1 Menu

Image 2.2 Installations

3. Main Menu – Application overview

Once the application is started, you will find yourself in front of the following menu.

Image 3.1 The Main Menu

Move the navigation key *up* and *down* to scroll over the items of the list. To make a selection you can either use the left soft key with label *Options* and then select *OK*, or push the navigation key which will take you directly to the next screen, depending on the item you selected.

To get some information about what you can do if you select some item of the list, click the right soft key (*Help)*. That would display a screen with information relative to the actions that you can make after you select the item of the list that was highlighted. For example, pressing the *Help* button while the screen looks like the picture in 3.2, would give you the screen that is shown in image 3.3 below.

Image 3.2 Help in the Main Menu

Help
Check the list of readers, manage SSL keys and certificates. Add a new reader or view the list of trusted Certification Authorities.
Back

Image 3.3 Help on Readers

To go back to the Main Menu, click the *Back* button. That will bring you to the exact same screen you could see before you press the *Help* button.

There are six items – options in the Main Menu. We will give a short description of each of them and what you can do after you select them. Each of the items is described in full details in one of the following sections of this manual.

3.1 Tags

After selecting the *Tag* item in the Main Menu, you can perform RFID *tag* related actions which include *Tag Key Management*, *Tag Spoofing* and *Management of Tag Lists*. Moreover, you can start RFID scans and also transfer ownership of tags between Guardians (*or users).

3.2 Readers

Selecting the *Readers* option will give you control over the RFID readers management. Besides being able to add and remove readers from the centralized Access Control List, you will be able to create/delete *Roles* for the readers, assign *Roles to Readers* and do *Key Management.*

3.3 Access Control

Under the *Access Control* option, you can select and set an ACL so that the Guardian will know how to behave against tags and readers. *Context* related operations are also available here. Finally, you can browse files on the Guardian side, and trasnfer them to your device.

3.4 Auditing

Auditing will give you all the important information of what has happened so far between the mobile device you use to control the RFID Guardian and the Guardian itself. This option has only informational pusposes.

3.5 Advanced

This option includes actions and operations that are considered advanced for the simple user. You should be careful when you are using some of the available operations in this section as you may cause irreversible damage to the RFID Guardian's or your mobile device's file system, lose some of your configuration changes to the ACL or compromise the security of the RFID Guardian (*what I mean here is if the user messes up with the keys or authentication)

3.6 Connect to Guardian

This option provides one of the most basic operations; the connection to the RFID Guardian over Bluetooth. This is usually what you would want to do first (connect to the Guardian), as a connection between the RFID Guardian and your device is necessary before you can do anything with the Guardian.

In the rest of this document, we describe one by one all the available options under the six items that were described above. We make the exception to start with the last one, as an established Bluetooth connection is necessary for the most of the operations of the other items. We continue with the rest of the items in the order they were described above and appear in the Main List of the application.

4. Connect to the RFID Guardian

All data between your mobile device and your RFID Guardian is sent over a Bluetooth communication channel. The connection establishment between the two devices is one of the first things you will have to do. Make sure you enable the *Bluetooth* on your device before you try any of the following. In case the *Bluetooth* is not enabled at the time you try to connect to the Guardian, you will get an error message. If so, exit the application, enable the *Bluetooth* on your device and try again.

Suppose the *Bluetooth* is enabled, go to *Main Menu > Connect to Guardian*. You will find yourself in front of the following screen:

Image 4.1 Bluetooth connection

Press the left soft key (*Start Search*) to start searching for *Bluetooth* enabled devices in your area. As long as a device is found, it will be added in a list in your screen. As most of the devices have a friendly name set by their user, this will be shown as default. In case no friendly name is assigned to a device, its MAC address will be shown (e.g *00-20-E0-6E-A3*-73). The picture in the left side of each device, indicates the type of the device (e.g computer, cellphone, etc).

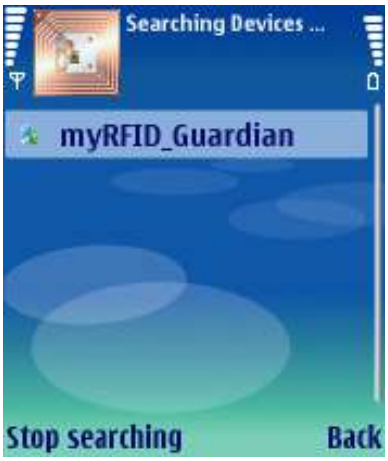


Image 4.2 Searching for Bluetooth devices

In busy places, it can be the case that the device search can last for a long time. For example, the application was tested outside an arrival terminal in Schiphol Airport, Amsterdam, and the search was not completed even after 7 minutes. In such cases, where there are a lot of devices nearby you (either crowded place or people who pass by) it is advisable to stop the search manually. That would save both time for you and battery for your device.

You can stop the search any time by pressing the left soft key (now with label *Stop searching*) while an inquiry is in progress. That would result in a screen similar to the following:

Image 4.3 Device search stopped

As long as the device discovery is stopped (either manually or automatically), you can select one of the devices to connect to. Make sure you select the right device e.g. your RFID Guardian device, to connect; otherwise it will not be possible to connect or even if a connection is established to another device, the application may stall, as your mobile device will be waiting for replies from the other device to requests it made, but were not handled correctly from the other device.

To connect to your RFID Guardian, navigate through the list of devices and once you are over the device you want to connect to, press *Options > Open connection*.

Image 4.4 Open connection to Bluetooth device

An attempt to connect to the selected device will be made. Wait until the connection is established.

Image 4.5 Connecting to a device

A message will let you know if the connection attempt was successful, and the *Main Menu* will be displayed. Now, you can continue with the rest of the options to interact with the RFID Guardian.

Image 4.6 Successful connection to a device

Once you are connected to a device, you can always disconnect by selecting *Main Menu > Connect to Guardian > Disconnect*. This option is only available when a connection is established. This is only the only available option under *Main Menu > Connect to Guardian* in this case, as multiple connections are not supported at the same time.

Note : In case you are asked to confirm that you "*allow the application to use connectivity applications*", click *Yes*. By clicking *No* you will not be able to connect to any device in later attempts, before you restart the application.

5. Tags

For tag related operations, go to *Main Menu > Tags*. From here you can do the following:

- Conduct an RFID scan (unimplemented)
- Transfer ownership of tags (unimplemented)
- Manage Tag Lists
- Do *key management*
- Do *tag spoofing*

The following picture shows the corresponding screenshot from the application:

Image 5.1 Tag options

5.1 Conduct RFID scan

To conduct an RFID scan, select *Main Menu > Tags > Conduct RFID scan*. [This is unimplemented now]

5.2 Transfer ownership of tags

To change the ownership of tags, select *Main Menu > Tags* > Ownership transfer. [This is unimplemented now]

5.3 Manage Tag Lists

Tag list management is available under (*Main Menu > Tags*) > Manage Tag Lists. You will be taken to the following screen, where you can

- Add / delete tags
- View the present tags in your vicinity
- View all the tags of the current Access Control List
- Create / delete / view sets of tags and assign tags to them

Image 5.2 Manage Tag Lists

Note : To be able to do all of the above, you need to specify an Access Control List directory first. See 7.1.1 “Select ACL directory” or select *Main List > Access Control* > ACL rules > Select ACL directory.

5.3.1 Set management

* Select *Options > View* (or just push the navigation button) when *Show Sets* is highlighted to expand the list of sets of the current ACL. To hide the list of sets, select Options > View when *Hide Sets* is highlighted.

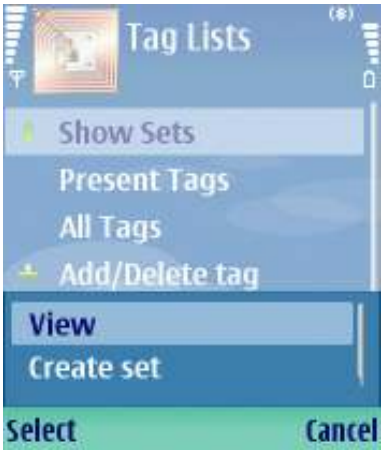


Image 5.3 Expand sets of tags

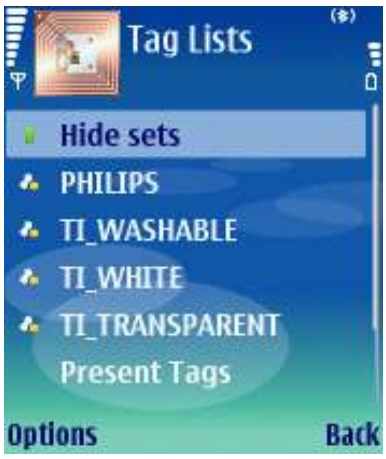


Image 5.4 Hide sets

* Select *Options > View* over a *set* to view its content. The list of tags that the set contains will appear (Image 5.5). To add more tags into the set, select *Options > Add a tag*. A list of all tags that *do not* belong to the set will be displayed (Image 5.6). Choose which tag(s) you want to add, and click *Options > Add to*

SET, where *SET* will be the name of the set you are editing (Image 5.7). To go back to the list of tags that the set contains, select *Back*. If some tags where added to the set, the new list will be displayed.

To delete some of the tags that belong to the set, choose which tag(s) you want to remove and select *Options > Delete from set* (Image 5.8). Multiple selection is allowed. If by mistake you deleted a tag, you can follow the instructions in the paragraph above to add it back to the set.

Image 5.5 Tags of set PHILIPS

Image 5.6 Tags that do not belong to PHILIPS

Image 5.7 Add tags to set

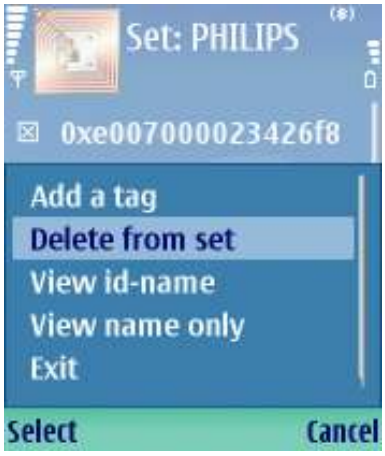


Image 5.8 Delete tags from set

By default, the name of the tag will be displayed in each list of tags. In case a tag does not have a name, its hexadecimal ID will be displayed. You can choose which information you want to see by selecting *Options > View id – name*, *Options > View id only* or *Options > View name only*.

Select *Back* when you are viewing the list of tags that belong to a set to go back to the screen where you can view all the sets of tags.

* To create a set of tags, select *Options > Create set*. You can either create an empty set by defining its name only, and then follow the instructions above to add some tags to it, or you can do that directly when creating the set. For the first option, define the name of the set, and then select *Options > Save* set. For the second option, select *Options > Add tags to set*. A list of all tags will be displayed and you can choose which tag(s) you want to include to your new defined set. After choosing the tags you want, select *Options > Save* set and you are done. Click *Back* to go to the previous screen. If you have saved your set, you can view it by expanding the list of sets (if not expanded already).

Image 5.9 Create a set with tags

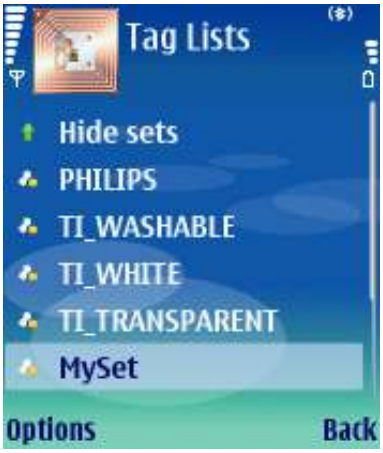


Image 5.10 Updated list of sets

* To delete a set of tags, the set has to be empty. First select to view the tags of the set you want to delete by selecting *Options > View*, and then remove all tags from the set. Then go back, and select *Options > Delete set*. If the set is empty it will be deleted. Otherwise an alert will be shown with some relative information.

5.3.2 *Present* Tags

Select *Options > View* over *Present Tags* to view the current tags in your vicinity. [This is unimplemented now]

5.3.3 *All* Tags

Select *Options > View* over *All Tags* to view all the tags of the current Access Control List. As it was mentioned before, the default representation of each tag is its name; if there is no name, its hexadecimal ID is presented.

It is possible to rename a tag. Choose which tag you want to rename from the list, and select *Options > Rename Tag*. That would bring you in front of a form with two fields. The first field holds the current name of the tag and it is editable. The second field holds the hexadecimal ID of the tag, and is not editable. Give a name to the tag and select *Options > Save changes*.

Image 5.11 Rename a tag

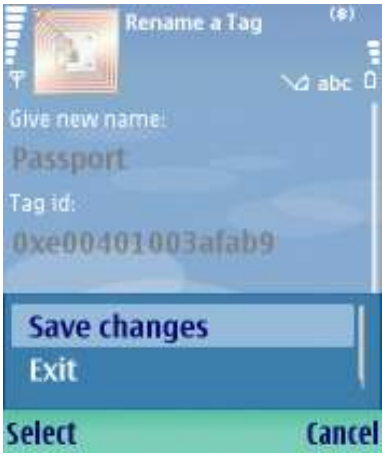


Image 5.12 Save renamed tag

Your tag has now a new name! Click *Back* to go to the list of all tags; you can now see your renamed tag.

Image 5.13 Renamed tag in global Tag list

Finally, you can add and delete tags in the global tag list. Simply select *Options > Add a tag* to add a tag (see 5.3.4 Add – Delete tags) or make a selection of tag(s) that you want to delete, and click *Options > Delete from set*. Note that it is not possible to delete tags from the global tag list, if they belong to some of the tag sets mentioned above.

Note : Renaming a tag is only possible through the Global Tag List. Any changes made here apply however to all sets. For example, if a set X includes the “tag A”, which is later renamed to “tag B”, the new name “tag B” will be displayed in the set X.

5.3.4 Add – Delete Tags

You can manually add and delete tags in the global tag list. To do that, select the *Add/Delete tag* option in *Main Menu > Tags > Manage Tag Lists*. To add a tag, you need to specify a unique name and a unique identification number. The ID of the tag has to be given in hexadecimal representation. An example is given below:

Image 5.14 Add a tag in the global tag list

To delete tags from the global tag list, you can specify the name of the tag you want to delete or its ID and then select *Options > Remove tag*. However, it is recommended and also easier to do it the way it was described in the previous section (see 5.3.3 All Tags).

5.4 Key management

Select *Main Menu > Tags > Key management*. A four-fielded form will appear; the default values for each field are shown in the following image:

5.15 Tag key management

From here it is possible to manage keys related to tags. A list of all tag sets is given and you may choose one of the sets, if you know which set your tag belongs to. Push the navigation button inside and the list of sets will appear. Select one tag set and click *OK*. Otherwise, leave the first field as it is.

5.16 Select set in Tag Key management

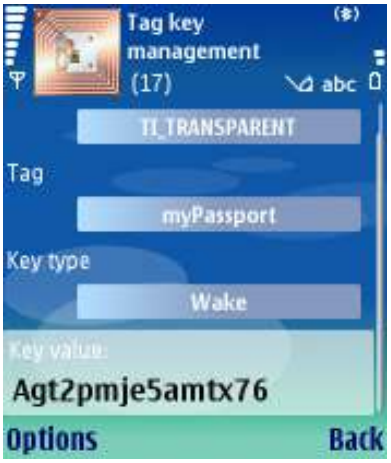
If you choose one of the sets, then the second field is updated to contain only those tags that belong to that set. Make your tag selection by pushing the navigation key over the second field (*Tag*) and then scrolling over the tag you want, in the list that will pop up. Then select *OK*.

5.17 Select tag in Tag Key management

If no *Tag set* was selected, then the *Tag* field contains all the tags. The procedure to select a tag is the same.

After you have selected a *Tag*, you have to specify what kind of key you want to set/modify. Once more, press the navigation key, this time when the *Key type* field is highlighted. Select the type of key you want to set, and click *OK*. Now you are ready to specify the value of that key in the field *Key value*. Once you do that, select *Options > Save* and your key will be saved / updated.

5.18 Select key type in Tag Key management



5.19 Specify key value

5.5 Tag spoofing

Select *Main Menu > Tags > Tag Spoofing*. To change the status of spoofing, click on the last item in the list *Spoofing: enabled*. Spoofing will be disabled or enabled respectively, depending on the current status.

Image 5.20 Tag Spoofing

To view and manage the list of spoofed tags, select *List spoofed tags*. The list of spoofed tags will appear. To add tags in this list, select *Options > Add spoofed tag* and you specify a name, block size and number of blocks for the tag to be added. An example is given here in picture 5.21.

Select *Options > Add tag* to add the tag in the list. If you click *Back*, you should see the new, spoofed tag in the list.

Image 5.21 Add spoofed tag

Image 5.22 Updated spoof list

Once you are in the list with the spoofed tags, you can choose one of them and then select *Options > Set spoofed tag* to set it. To see the set spoofed tag(s), simply select *Options > Get spoofed tag*. A pop up window will inform you for the current spoofed tag(s).

(*the above text will probably be removed, right?)

To remove a spoofed tag, you can either do it by selecting *Remove spoofed tag* from the Spoofed Tags menu, or enter the list with the spoofed tags, choose which ones you want to remove and then select *Options > Remove Selected*. Use the first option if you know the ID of the tag you want to remove and the list of the spoofed tags is long. Use the second method if you want to delete more than one tags in one go.

6. Readers

For reader related operations, go to *Main Menu > Readers*. Here you have the following options:

- Manage Reader Lists
- Manage Role Lists
- Do *key management*
- Add / remove Readers
- Add / remove Roles

The following picture shows the corresponding screenshot from the application:

Image 6.1 Reader options

6.1 List of Readers

Select *Main Menu > Readers > List of Readers*. The list you see is the list of all readers in the current Access Control List. What you can do here is:

- Add a reader
- Delete a reader
- View roles of a reader and add new roles to it
- Set a reader as current reader
- Check who the current reader is

Image 6.2 List or readers

Image 6.3 Options in List of readers

* To add a new reader, select *Options > Add a reader*. All you have to specify is the readers name (* is this how it is going to work eventually?). Give the name of the reader and select *Options > Add reader*.Then select *Back* to see the new list with the readers, including the one you just added.

* To delete a reader, you have to choose from the list of readers which readers you want to remove, and then select *Options > Delete Selected*. Multiple selections is allowed. Notice, however, that deleting a reader is only possible if the reader is *role-free*, that is, it has no role(s) assigned with it.

* You can manually set a reader as the *current* reader. To do that, choose which reader you want to set, and select *Options > Set as current*.

* To view the current reader, simply select *Options > Show current reader*. It doesn't matter whether any reader is selected from the list in this case.

Readers and roles are closely related. A reader can have one or more roles; moreover, a role can be given to one or more readers. As the relation between readers and roles is *m to n*, it is was necessary to be able to manage readers and roles from both points of view. At this point, you can manage which roles a reader may have. See *6.2 List of Roles* to set which readers a role may be given to.

* To view the roles of a reader, choose a reader from the list of ACL readers and select *Options > View roles*. The list of roles, that the reader you selected, has, will be shown. You can always check the title of the screen to make sure what kind of list you are viewing. Select *Options > Add more roles* if you want to give your reader more roles. A list of roles that your reader *does not* have will be given. Make your selection and then click *Options > Add roles to READER*, where READER will be the name of your reader. An example is given below to make the procedure more clear.

Likewise, to delete roles from a reader, select some of the roles that your reader already supports, and then select *Options > Remove selected roles*. You can always give back to your reader those roles you have just deleted by following the instructions in the previous paragraph. The roles you have just deleted will now appear in the list of roles, after you have selected *Options > Add more roles*.

Image 6.4 View roles not supported by a reader

Image 6.5 Add selected roles to reader

* You can also add roles to your reader without having to view the roles of the reader first. Select *Options > Add roles* and then continue as described above.

6.2 List of Roles

Select *Main Menu > Readers > List of Roles* to view the list of Roles of the current Access Control List. What you can do here is:

- Create – delete roles
- View roles of readers and
- Give new roles to readers or delete roles from them

All these options are available under *Options*, as shown in the following picture.

Image 6.6 List of roles

Image 6.7 Available options for roles

* To create a role, select *Options > Create role*. In the form that you seen now, specify a name for your role and then select *Options > Create role* again. It is also possible to delete a role from here, by specifying the name of it, and selecting *Options > Delete role*. This is only possible if the role is *reader-free*, that is, the role is not given to any reader.

* Another, easier in some cases way to delete roles, is by making a selection of roles in the list of ACL Roles, and then select *Options > Remove selected*. Multiple choice of roles is allowed and makes the process faster, but once again, the role(s) has to be *reader-free*.

* To give a role to some readers of the ACL, select a role and then press *Options > Assign to readers* (Image 6.8). That would bring you the list of readers that do not have the role you selected (Image 6.9). Choose some of the readers (if any) from the list, and then select *Options > Add selected*. Now those readers have the role you specified.

* In case you want to check which readers have some specific role, choose this role that you are interested in, and then select *Options > List members of role*. All those readers that you see now have the role you chose (Image 6.10). You can also add readers to this role, by selecting *Options > Add more readers* (Image 6.11) or delete some of the readers, by choosing some readers from the list and selecting *Options > Remove selected*.

Image 6.8 Add readers to a role

Image 6.9 Readers without the role

Note : The resulting list of readers you get by selecting a role and then *Options > Assign to readers*, will always be the same with the resulting list, if you select the same role, then *Options > List members of role*, and then in the new screen *Options > Add more readers*.

Image 6.10 FRIENDLY_READERS

Image 6.11 Add more to this role

In the example above we selected to view the *list of members* of the role FRIENDLY_READERS. Then we decided to *add more readers* to this role. We selected all the readers that did not have this role, and *added* them. The updated list of FRIENDLY_READERS after that, looked like the one in Image 6.12.

Image 6.12 New list of readers

6.3 Key management

Select *Main Menu > Readers > Key management* to manage keys related to readers. Key management is divided in two categories here, depending on the type of the key. Therefor, there are two options:

- Assymetric Key management
- Symmetric Key management

[This is not yet implemented]

6.4 Add/Remove reader

Select *Main Menu > Readers > Add/Remove reader*.

This is actually a shortcut to the form we mentioned before, where you can add and delete readers by specifying their name. See *6.1 List of Readers*, *Options > Add a reader*, for more details.

6.5 Create/Delete role

Select *Main Menu > Readers > Create/Delete role*.

Similar to the previous section, this is a shortcut to the form where you can create/delete roles. See *6.2 List of Roles*, *Options > Create role*, for more details.

7. Access Control

An Access Control List basically describes the rules according to which the RFID Guardian operates. The relation between tags, readers and roles is fully described in the ACL. An RFID Guardian may also operate under different contexts, set by the user. To manage ACLs or contexts, select *Main Menu > Access Control > ACL rules* (see *7.1 ACL rules*) or *Main Menu > Access Control > Context* (see *7.2 Context*) respectively.

Image 7.1 Access Control

7.1 Access Control List rules (ACL rules)

7.1.1 Select ACL directory

It is usually the case, that after connecting to your RFID Guardian, you will want to specify an Access Control List according to which your Guardian will operate. To do so, you will have to browse through the Guardian's file system, and choose an ACL. Select the first option in the list with the ACL rules, *Select ACL directory*. You will be given the list of files and folders of the default directory of your Guardian.

Image 7.2 ACL Rules

Image 7.3 Guardian files

To go one directory up, you have to select the two dots "..".The default action when pressing the navigation button here, depends on the item that is highlighted. If this is a file, then pressing the navigation button will open the file; if it is a folder, then it will browse the content of the folder. The same happens when you select *Options > Enter*. If you try to enter a file, the file's content will be displayed, whereas if you try to enter a folder, the folder's content will be listed. To exit the Guardian browser, you can select the *Exit browser* option, which always appears over the right soft key. That will bring you to the screen shown in image 7.2.

Navigate through the Guardian's file system to find the directory that you want to set as your *acl directory*. Once you find it, you have two options on how to set it. First, you can enter the directory and then select *Options > Set acl directory* over the single dot ".". That means that you set the current directory as your *acl directory*. The other option is to select *Options > Set acl directory* without entering the directory. However, the directory that you want to set should be highlighted again. If the directory that you are trying to set is not a valid one, you will receive an error alert. Otherwise, you will a confirmation alert will be displayed.

There are certain other options available when you are browsing the files of your Guardian, similar to any other operating systems file system. For example, you can create your own directories by selecting *Options > Create directory*. Moreover, you can delete directories as long as they are emtpy, by selecting *Options > Remove directory*. To delete a file, you must select *Options > Delete file* over the file that you want to delete.

Creating a file on the Guardian is only available in the case where you transfer a file from your mobile device to the Guardian (upload). We discuss this later in *9.3.6 Phone Browser* [this will probably change].

The list of all options described above is given in the following picture:

Image 7.4 Options in Guardian browser

Note : To avoid confusion when browsing the files of the Guardian and the files of the mobile device, yellow folders are used in the Guardian browser, while green ones are used in the phone browser.

7.1.2 Check ACL status

It is possible to view information about the current state of the Access Control, that your Guardian operates according to. Select *Check ACL status* and a form with all available information will be shown. You can see which the current reader is, the current context and the current ACL directory for example. An example is given in the following two pictures:

Images 7.5, 7.6 ACL status information

This form provides only information and cannot be changed, e.g you cannot change the current reader from here. For this reason, there is only a *Back* button, that will bring you to the previous menu (see image 7.2)

** [I need to know here exactly what is what, so that I describe better if necessary]

7.1.3 ACL reload

Select this option, *ACL reload*, if after you made some changes to the Access Control List that you loaded, you want to undo them. For example, suppose you changed the current reader, or deleted some roles, or anything similar to that. Reloading the ACL, will put away all these changes and bring the ACL to its original state.

7.1.4 ACL save

[not implemented! Maybe this option will be removed]

7.1.5 Clear ACL

To clear the current ACL, select *Clear ACL*. After that, there is no ACL loaded. To load an ACL see *7.1.1 Select acl directory*.

7.2 ACL Contexts

A context can be imagined as a mode of operation or a profile. Similar to the *General, Silent* or *Meeting* profiles on Nokia devices, where you actually specify the area you are currently in and how your mobile device should operate, you can do the same for the Guardian, by specifying an *Indoor*, *General* or any other context.

To view the current contexts, select *List Contexts*. A list of the existing contexts will appear. You can create your own context, by selecting *Options > Add new context*. Specify a name for the context in the form that you will see and then select *Options > Add context*.

Image 7.7 Add a context to the ACL

To delete a context from the context list, make your selection and then click *Options > Remove Selected*. Set a context as the current context (active) by choosing it from the list and then selecting *Options > Set as current*. To view the current context, select *Options > Show current context*. This information should be of course the same with the one you get in the *Current context* field of the ACL status form, described above in 7.2 (Image 7.5).

Image 7.8 List of contexts

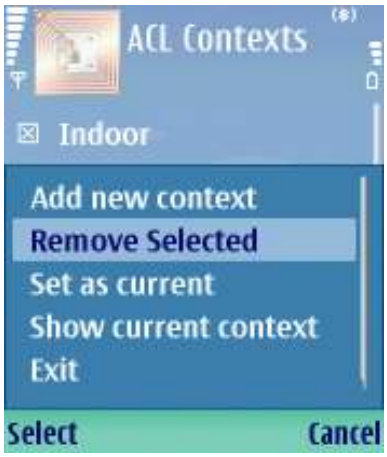


Image 7.9 Removing contexts

8. Auditing

Communication between the Guardian and your mobile device is logged, so that you can actually check exaclty what kind of actions were performed. This here is not the same with the auditing functionality that the RFID Guardian itself supports.

There are four different types of logs:

- the Real time alerts log
- the Tag log
- the Scan log
- and the general (action) log

Image 8.1 Logs

For the time being, everything is logged in the *action* log. A typical example of what is logged in there is shown in the next pictures. The log is divided in pages, to make it easier to view. Each page of the log will keep up to 10 messages.

Images 8.2, 8.3 Log examples

To view the next or previous page of the log, either push the navigation button and select *Next Page* or *Previous Page*, or select *Options > Next Page*, *Options > Previous Page* respectively.

If there is some kind of communication between the Guardian and your device at the time you are viewing the log, you can select the *Options > Refresh* option to update the log file. Any new messages will appear in the log.

Finally, to delete the log select *Options > Delete*. Notice that the whole log will be cleared, and not only the current page of the log that you are viewing.

Image 8.4 Log options

** [we should discuss about how to organise the log thing better, what kind of things to log to each of the log files, make a copy on the phone or keep it temporary as long as the application is running, etc...]

9. Advanced

Select *Main Menu > Advanced*. Operations that belong to this section are considered advanced for the simple user and the user is supposed to know what he is about to do with the Guardian. All available operations are divided in three categories, depending on what they are actually about. The advanced operations are thus devided into:

- Security
- Configuration and
- Administration

Image 9.1 Advanced categories

9.1 Security

Select *Main Menu > Advanced > Security*.

Not much is working here. Right now we have options like Fuzzing, Relay and Replay attacks, and Eavesdropping on tag responses. There is no actuall functionality though at this moment.

9.2 Configuration

Select *Main Menu > Advanced > Configuration*.

From this point here, you can configure different settings of the RFID Guardian. The list of options you have is:

- do authentication
- do Key management
- change the Access Control
- manage Auditing
- change the System's time

9.2.1 Authentication

Select *Main Menu > Advanced > Configuration > Authentication*.

This part is not implemented yet. What exactly are we supposed to implement?

9.2.2 Key management

Select *Main Menu > Advanced > Configuration > Key management*.

Also not implemented! What should be added here?

9.2.3 Access Control

Select *Main Menu > Advanced > Configuration > Access Control*.

Not implemented! Add what in here?

9.2.4 Auditing

Select *Main Menu > Advanced > Configuration > Auditing*.

Auditing is necessary for the enforcement of RFID security policies and also provides proof of activity to the user. However, the user is given control over auditing, and can disable it, as well as enable it at any time.

Requests to the RFID Guardian and responses from it can be seperately handled with respect to auditing. It is possible that you audit only requests, and do not log the responses to these requests. Press the navigation button when you are over the item of the list that you want to change its state. Press again to bring it to its original state. The same result can come by selecting *Options > Change*.

As long as auditing is enabled, you can furthermore choose whether you want to log tag related action, or scan related one. To change the current state of logging, press the navigation button when the desired item is highlighted.

The third item in the list shows the file where requests and responses are logged. Tag and scan logging however, takes place in different files, as described in *8. Auditing*.

9.2.5 System time

Select *Main Menu > Advanced > Configuration > System time*.

This is where you can change the time of your RFID Guardian from. A simple field like the one shown in the next picture holds the current time and date of your RFID Guardian. Move the navigation button to the left or right to select the part that you want to change. Then type in the value that you want. When you are finished, select *Options > Save* to apply your changes to the Guardian.

Image 9.2 Change the system time

9.3 Administration

Select *Main Menu > Advanced > Administration*.

You have the options to:

- Load new programs to the Guardian (?)
- reflash its EEPROM
- Clean up its filesystem
- Backup
- Synchronize
- browse your mobile's device file system and upload files to the RFID Guardian
- browse your RFID Guardian's file system and download files to your mobile device.

Most of those options are shown in the next picture:

Image 9.3 Administration options

9.3.1 Load new programs

Select *Main Menu > Advanced > Administration > Load new programs*.

This is unimplemented. What should be here anyway?

9.3.2 Reflash EEPROM

Select *Main Menu > Advanced > Administration > reflash EEPROM*.

Unimplemented!!

9.3.3 Clean up the filesystem

Select *Main Menu > Advanced > Administration > Clean up filesystem*.

UNIMPLEMENTED!!!

9.3.4 Backup

Select *Main Menu > Advanced > Administration > Backup*.

UnImPlEmEnTeD!

9.3.5 Synchronize

Select *Main Menu > Advanced > Administration > Synchronization*.

uNiMpLeMeNtEd!

9.3.6 Phone Browser

Select *Main Menu > Advanced > Administration > Phone browser*.

This will put you in front of the local file system on your device. You may be asked whether you allow the application to read user data; in this case you should say *Yes*. The purpose of the *Phone Browser* is that it allows you to transfer files from your mobile device directly to the RFID Guardian. Those files you may create and modify even if you are not connected to the Guardian, and upload later. You can also view and edit downloaded files from the Guardian.

Navigate through the device's file system. Either push the navigation button to enter a folder or select *Options > Open*. The local file system is more or less presented the same way as the RFID Guardian's file system is. Navigation into it also adheres to the same rules like in the Guardian's file system. However, there are some different options in the *Phone Browser*.

Image 9.4 Phone browser

Image 9.5 Phone browser options

* To upload a file to the Guardian, go over the file that you want and select *Options > Upload to Guardian*. That would bring you now in the RFID Guardian's file system, where you would have to select where and under which name you want to save the file. For your convinience and to avoid confusion, the folders in the Phone browser are green, while they are yellow in the Guardian browser.

Once you have selected to upload a file to the Guardian, two more options are added to the Guardian browser, compared to those shown in image *7.4 Options in Guardian browser*. Now, you can select the *Save here* or the *Save in new file* option, under *Options*. The first one would overwrite the highlighetd file in the Guardian browser with the file that you are uploading. The second option, will create a new file in the Guardian side, with the same name like the file's that you upload. Once you have selected to save the file in the Guardian, the two extra options will disappear from the *Options* menu.

* Select *Options > Properties* over a file or a folder to view the related properties of this entity. An example is given in the following pictures, where the properties of the file *Ajt* are displayed:

Images 9.6, 9.7 Properties of a file

* To view a file from the Phone browser, select *Options > Open*. Then select *Back* to go back to the browser, or *Exit browser* to go to the Administration menu.

* To create a file or a folder on the Phone, select *Options > New*. Specify a name in the form that will be displayed and select whether you want to create a file or a folder. Then select *Options > OK* to create your file or directory. Here is an example, where a file is created:

Image 9.8 Create a file on the phone

* To delete a file or a folder, select *Options > Delete*. Folders can only be deleted if they are empty.

9.3.7 Guardian Browser

Select *Main Menu > Advanced > Administration > Guardian browser*.

You have already seen some of what is available here, in section *7.1.1 Select ACL directory*. Most of the available options were discussed in this section. However, almost nothing was said for the case where you open a file to view. To view a file, you have to select *Options > Enter* over a file. That would open an editor with the content of the selected file, as shown in the next picture.

Image 9.9 Viewing a file

There is an option that allows you to download the file that you view, to your mobile device. Select *Options > Download to phone* and you will be taken to the Phone browser. Choose the directory where you want to save this file, and either select *Options > Save here* over an existing file to overwrite it, or select *Option > New*, create a file with some name as discussed in *9.3.6 Phone Browser* and then select *Options > Save* over that file you just created.

If you press the *Exit browser* button, you will exit the Phone browser, and you will be taken back to the open file that you copied from the Guardian side. Click *Back* to close the file and go to the Guardian browser.

Note : The Save here command in the Phone browser becomes available only after you select to download a file from the Guardian to the phone, and disappears after the file is downloaded.